Date of Hearing: May 9, 2011

ASSEMBLY COMMITTEE ON BANKING AND FINANCE
Mike Eng, Chair
AB 1080 (Calderon) – As Amended: May 4, 2011

SUBJECT: Internet transactions: verification: banking and financial services.

SUMMARY: Requires businesses that provide banking and other financial services to post specified information on their Internet Web site. Specifically, this bill:

1) Provides that a business that provides banking and other financial services and allows for the movement of funds under the ownership and control of a person or business over the internet to collect and report, on an annual basis, the following information:

   a) The number of instances in which an unauthorized transfer of funds occurred over the internet; and,

   b) The total sum of unauthorized funds transferred over the Internet.

2) Specifies the collection of the statistics is limited to customers affected in California.

3) Requires the bank or financial institution to post the report on their Internet Web site.

EXSITING FEDERAL LAW

1) Establishes Regulation E, the Electronic Fund Transfer Act to establish the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. The primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers. (*12* C.F.R. § 205.1)

2) Requires banks, savings associations, and credit unions to verify the identity of customers opening new accounts. (See e.g. 31 CFR Section 103.121, implementing section 326 of the USA PATRIOT Act, 31 USC Section 5318(l).)

3) Requires banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family, or household purposes, with whom the institution has a continuing relationship. (See Interagency Guidelines Establishing Information Security Standards, implementing section 501(b) of the Gramm-Leach-Bliley Act, 15 USC 6801.)

EXISTING STATE LAW

1) Requires any agency, person, or business that owns or licenses computerized data that includes personal information to disclose a breach of the security of the system to any California resident whose unencrypted personal information was, or is reasonably believed to

have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civil Code Section 1798.82(a) and (c))

2) Requires any agency, person, or business that maintains computerized data that includes personal information that the agency, person, or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Civil Code Section 1798.82(b))

3) Defines "breach of the security of the system" as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. (Civil Code Section, 1798.82 (d))

4) Requires an agency, person, or business to provide breach notification using either written notice, electronic notice, or substitute notice. An entity may use substitute notice when it demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of persons to be notified exceeds 500,000, or if the entity does not have sufficient contact information. Substitute notice must consist of: (a) email notice when the entity has an email address for the affected individuals; (b) conspicuous posting of the notice on the entity's Web site; and (c) notification to major statewide media. (Civil Code Section 1798.82(g).)

5) Requires commercial Web site operators and online services that collect personally identifiable information about California residents to conspicuously post their privacy policy on their Web site, or in the case of an online service, to make that policy available to the public. (Business & Professions Code Section 22575.)

6) Makes it unlawful to knowingly access and, without permission, alter, damage, delete, destroy, or otherwise use any data, computer, computer system, or compute network to (1) devise or execute a scheme to fraud or extort, or (2) wrongfully control or obtain money, property, or data. (Penal Code Section 502.)

7) Makes it unlawful to willfully use someone else's personal identifying information for an unlawful purpose, including obtaining or attempting to obtain credit, goods, services, or medical information in the name of the other person without that person's consent. (Penal Code Section 530.5.)

FISCAL EFFECT: None.

COMMENTS:

This measure attempts to bring more awareness to the issue of cyber-attacks and the amount of money taken from consumers through the fraudulent transfer of funds.

Under existing law, a person, business, or state agency that keeps, maintains, or leases computerized data that contains personal information must notify anyone whose personal

information is compromised as a result of a data breach. The law permits the person, business, or state agency to use "substitute notice" if the number of persons affected would make personal notice prohibitively expensive or impractical, or if the affected person's contact information is not available. Existing law does not require banks or financial institutions to post specific data required in this measure on their Internet Web site. Most, if not all of the businesses that fall under this measure already have an area on their website where consumers can go to report and find out more information on fraud. The statistics requested under this measure would let consumers know how many times an unauthorized transfer of funds occurred at that business and the amount of money transferred unauthorized.

This measure would encompass insurance companies, credit card companies, banks, credit unions, community banks, commercial banks, payday lenders, consumer finance companies, investment funds, and stock brokerages. A number of these institutions are nationwide, considering the measure only applies to California residents, an institution would be required to conspicuously post on their website information based on those California residents who have had unauthorized transfer of funds.

The safety of consumer's personal information has come under recent scrutiny because of the hacking of Sony Playstation Network. Approximately 100 million accounts worldwide may have been compromised through this data breach. Sony is being scrutinized for the lack of prompt notification which is getting the attention of the federal government. Sony realized on April 19, 2011 that their system had a data breach but did not email consumers who may have been affected until April 26, 2011. Sony has stated it will cover the cost of reissuing new credit cards if affected users choose to do so and they will also pay for credit card insurance programs on a region and case by case basis. It seems lawmakers in Washington D.C. may press for legislation that will require more timely and complete notification when such intrusions occur. AB 1080 would not apply to this incident since Sony is not considered a business that provides banking or other financial services.

CONCERNS:

While the Author has good intentions with this measure, requiring businesses to post the specified data on the Internet in a conspicuous manner may actually provide more harm than help. This information could actually be used as a tool for hackers. In reality, hackers could visit the Internet Websites of all the institutions required to do this and compare and view which financial institutions have the weakest security infrastructure. This may put these businesses at more risk than is necessary. Existing law already provides that a consumer is made aware of a breach through notification; SB 24 is currently moving through the legislative process which would expand on what is included in the notification, discussed below.

RELATED LEGISLATION:

SB 24 (Simitian, 2011 Legislative Session) This bill amends California's security breach notification law to provide that any agency, person, or business required to issue a notification under existing law must meet additional requirements regarding that notification. This bill requires that security breach notifications be written in plain language and contain certain specified information, including, among other things, contact information regarding the breach,

the types of information breached, and, if possible to determine, the date, estimated date, or date range of the breach. This bill provides that a security breach notification may also include other specified information, at the discretion of the entity issuing the notification. This bill requires that, any agency, person, or business that must provide a security breach notification under existing law to more than 500 California residents as a result of a single breach would be required to submit the notification electronically to the Attorney General. Pending in Assembly Judiciary.

PREVIOUS LEGISLATION:

AB 230 (Calderon, 2010 Legislative Session) would require a business that provides banking or other financial services over the Internet to implement and maintain-reasonable policies and procedures for authenticating and verifying- the legitimacy of a consumer transaction over the Internet. The bill would authorize the imposition of a civil-penalty and a civil action. Withdrawn from Senate Judiciary without further action.

SB 1166 (Simitian, 2010 Legislative Session), would have amended California's security breach notification law to provide that any agency, person, or business required to issue a notification under existing law must meet additional requirements regarding that notification. This bill would have required that security breach notifications be written in plain language and contain certain specified information, including contact information regarding the breach, the types of information breached, and the date, estimated date, or date range of the breach. This bill would provide that a security breach notification may also include other specified information, at the discretion of the entity issuing the notification. This bill was vetoed.

SB 20 (Simitian, 2009 Legislative Session) would have required that breach notifications be written in plain language and contain specified information. This bill was vetoed.

SB 364 (Simitian, 2008 Legislative Session) would have established additional notification requirements following a security breach of a computerized data system. The bill was vetoed.

AB 1656 (Jones, 2008 Legislative Session) This bill would have prohibited specified entities that sell goods or services from storing or failing to limit access to payment related information unless a specified exception applies. The bill was vetoed.

AB 1677(Calderon, 2007 Legislative Session) would require a business that provides banking or other financial services over the Internet to implement and maintain reasonable policies and procedures for authenticating and verifying the legitimacy of a consumer transaction over the Internet, and would require that these policies and-procedures be consistent with current best industry practices. It would allow penalties to be imposed on businesses that fail to meet this requirement. Moved t o inactive.

SB 1386 (Peace, Chapter 915 of 2002 Legislative Session) requires state agencies and businesses that own or license computerized data that includes personal information to disclose, as specified, any breach of security of the systems, as defined, to any California resident whose unencrypted personal information was, or may have been, acquired by an unauthorized person. It authorizes any customer injured by a failure to report to sue such entity

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

April 25, 2011 Version of Bill

American Express
California Bankers Association
California Chamber of Commerce
California Credit Union League
California Financial Services Association
California Independent Bankers
California Mortgage Bankers Association
California Retailers Association
National Business Coalition
State Farm

Analysis Prepared by: Kathleen O'Malley / B. & F. / (916) 319-3081